CorreLog®

SNMP Trap Monitor Software

Users Manual

http://www.correlog.com mailto:info@correlog.com

CorreLog, SNMP Trap Monitor Software Manual

Copyright © 2008 - 2015, CorreLog, Inc. All rights reserved.

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.

Table of Contents

Section 1: Introduction …….. 5

Section 2: Software Installation …….. 9

Section 3: Software Operation …….. 13

Alphabetical Index …….. 21

Section 1: Introduction

This manual provides a detailed description of the CorreLog SNMP Trap Monitor software. This is an optional set of files and executables added to the CorreLog Server order to expand the role of the CorreLog to include monitoring of standard SNMP traps.

The manual provides information on specific features and capabilities of this special software, including installation procedures, operating theory, application notes, and certain features not documented elsewhere.

The SNMP Trap Monitor software consists of several components. A background process continuously listens for SNMP traps, and converts these traps to syslog messages, which are sent to the CorreLog Server program. Additionally, a configuration screen is provided (under the "Messages > Config" tab) that permits the user to adjust the parameters of the background process. These components are described in detail within this document.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog system's role within an enterprise to include SNMP trap monitoring.

Overview Of Operation

The SNMP Trap Monitor software extends the CorreLog system to permit reception of SNMP traps. This allows CorreLog to actively monitor network devices that issue SNMP traps, including UNIX devices, Windows platforms, and network routers.

The CorreLog Trap Monitor "CO-systrap.exe" background process continuously listens for traps at the standard UDP port number of 162. When a trap is received (that matches certain user defined criteria) the "CO-systrap.exe" program composes a syslog message, and then sends this message to the CorreLog server. This gives CorreLog more awareness of the network and enterprise state.

The CorreLog SNMP Trap Monitor background process is configured and monitored using a tightly coupled integration with the main CorreLog web interface. The user configures one of several possible message formats, and provides basic information to filter incoming traps, such as the trap community name, and other criteria.

SNMP Trap Basics

SNMP traps are a standard message format, issued by a variety of different devices, which are typically used to indicate state changes and other information. Each SNMP trap is an encoded (non-human readable) message that contains the sending IP address, a numeric identifier of the trap type, an indicator of the general system (or sub-system) type, and various arguments. These components are described below.

- **IP Address.** Each SNMP trap contains the IP address of the related device (which may be different from the IP address of the device that sends the trap.) This IP address indicates the affected or associated network device that is the subject of the trap.

- **Community Name.** Each SNMP trap contains a user-defined password. This password is referred to (in the nomenclature of SNMP) as a "Trap Community Name", and can be used by CorreLog to limit the range of traps to a specific group of devices that know the configured trap community name of the CorreLog server. (By default, CorreLog accepts any trap community name, unless this configuration is specifically changed as discussed in later sections.)

- **Enterprise OID**. Each SNMP trap contains an identifier of the system or subsystem related to the trap. This is referred to (in the nomenclature of SNMP) as the "Object Identifier" or OID. The Enterprise OID and trap number (described below) uniquely identify the SNMP trap in the universe

of possible traps. CorreLog automatically translates the Enterprise OID into a human readable description.

- **Trap Number.** Each SNMP trap contains a trap number that identifies the trap type. These trap numbers identify "coldstart", "warmstart', "linkup", "linkdown", "authentication", "neighbor loss" and "enterprise" traps. In particular, the "enterprise" trap can be extended to include any number of vendor specific traps, each identified with a second number.

- **Variable Bindings.** Each SNMP trap can contain zero or more additional pieces of information. This additional information is referred to (in the nomenclature of SNMP) as a "Variable Binding", where each variable binding contains an arbitrary binding object and value. CorreLog automatically formats variable bindings into a single human-readable message.

The network device controls the actual SNMP trap transmission, and the administrator should configure each managed device with a "Trap Destination" and "Trap Community" value. The specific details of this configuration process vary, and depend upon the network device type and vendor instructions.

A large amount of information exists related to SNMP network management. A detailed discussion of all aspects of SNMP trap reception is beyond the scope of this manual. Users should consult third-party documentation for more detailed information, or contact CorreLog for training.

SNMP Trap Monitor System Software Components

The CorreLog SNMP Trap software comes as a single downloadable package in self-extracting WinZip format. This package is installed at the CorreLog server, and contains the following specific components.

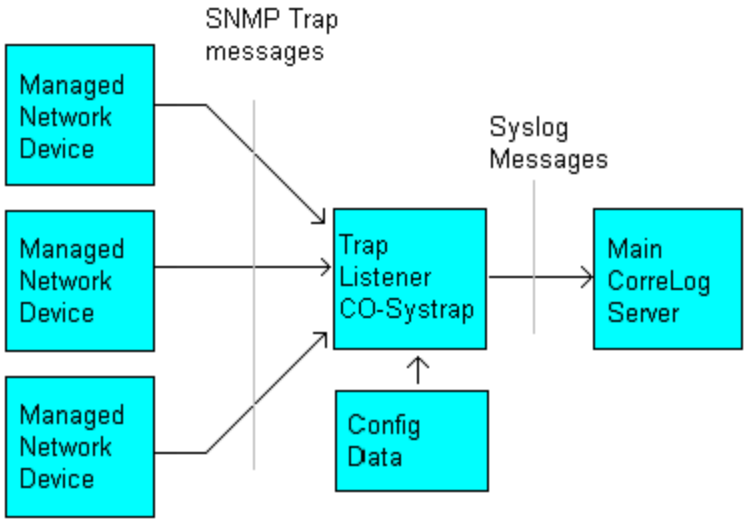
- **CO-systrap.exe Program.** This is the trap listening process that is responsible for receiving an SNMP trap, converting the message to syslog format, and resending the trap to CorreLog. The process is configured to start on the "System > Schedule" screen, documented in later sections.

- **Configuration Screen.** This is a support screen, available under the "Messages > Config > Traps" tab of the CorreLog web interface as part of the Windows component installation. This screen allows the operator to configure the various parameters related to the SNMP trap reception.

- **Configuration Data.** This is ancillary data that is used by the SNMP trap process, such as a list of Enterprise OIDs and their corresponding human readable names. This data can be modified by the end-user, discussed in later sections.

System Block Diagram

The CorreLog SNMP Trap Monitor process consists of a single background process. This process reads configuration data that has been specified by the operator. The process awaits reception of SNMP trap messages. When a device sends an SNMP trap, the trap is converted to a syslog message and then sent to the CorreLog server. A simple block diagram of this operation is depicted below.



As indicated in the above diagram, the CO-Systrap.exe process (installed and configured as described in the next chapters) continuously listens for SNMP traps issued from network devices. These devices can be Windows platforms, UNIX servers, Routers, Switches, and other network equipment. The background process is completely controlled and by data that is configured by the operator using the "Messages > Config > Traps" screen of the Main CorreLog Server web interface.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install the CorreLog Trap Monitor software. Note that the only required components of the system are the CO-sytrap.exe program and the Trap configuration screen, documented herein. Other information on the CorreLog server can be found in the standard "User Manual", including operation and application notes that will be of assistance in processing the SNMP Trap messages received by the main CorreLog Server.

Section 2: Software Installation

The CorreLog SNMP Trap Monitor software is usually delivered as a self-extracting WinZip file. The installation requires a few simple manual installation steps, and no automatic installation is provided or required. The basic installation steps are as follows:

1. The user obtains the CorreLog SNMP Trap Monitor software, in self-extracting WinZip format.

2. The user stops the CorreLog Server "Framework Service", and verifies via the task manager that all CorreLog background processes have stopped.

3. The user executes the self-extracting WinZip file. This unzips the software into the CorreLog Windows Distribution, including all configuration data and executables, and modifies the CorreLog program to start the background processes on system startup.

4. The user restarts CorreLog, and optionally configures parameters via the "Messages > Config > Traps" screen.

5. The user configures other parts of the CorreLog system, such as Threads, Alerts, and Ticket users, to correlate and process the syslog messages that are generated by the new software.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

- **Existing CorreLog Server Installation.** Prior to installing the software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Disk Space Requirements.** The SNMP Trap Monitor software requires no significant disk space beyond the normal footprint of the CorreLog server. There is generally no extra disk space load due to this software.

- **CPU Requirements**. The SNMP Trap Monitor software requires very little extra CPU requirements. A single process is started the CorreLog Windows platform, which consumes minimal CPU resources.

- **Firewall Requirements.** The SNMP Trap Monitor software requires that managed devices can access the CorreLog Server through the standard SNMP UDP port of 162. This may be a normal condition (however some sites may purposely disable this port, and those selected devices will not be manageable by CorreLog.)

To insure proper installation of the program, the user should close all windows, and temporarily disable any port blocking or Virus Scan software on the system. The existing CorreLog server process should be stopped prior to the installation. Reboot, after installation, is not required.

Windows Installation Procedure

The specific steps needed to install the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Stop the CorreLog Server processes via the Windows Service Manager, or via the "Start and Stop Services" utility found in the Windows Start menu. Verify with the Windows "Task Manager" that all CorreLog processes are stopped.

3. Obtain and execute the "co-n-n-n-trap.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog"). After extracting files, the "About" dialog is displayed indicating the success of the installation.

   Comment: After extracting files, the installer will modify the CorreLog "Schedule" facility (in the "System" tab) to automatically start the background process: CO-systrap.exe" program on system startup.

4. Restart the CorreLog system processes via the Windows Service Manager or via the "Start and Stop Services" utility.

5. Verify with the Windows "Task Manager" that the "CO-systrap.exe" process is now running on the system.

SNMP Trap Monitor Configuration

Once the CO-systrap.exe program has been installed and is running on the system, the user can configure parameters associated with the background process. The user accomplishes this activity via the "Messages > Config > Traps" screen. (This tab is automatically added to your system, if it does not already exist.)

Additionally, the administrator should go to each device that will be sending traps to CorreLog, and direct the "Trap Destination" value to be the IP address of the CorreLog server. Additionally, the administrator can select a standard "Trap Community" value that can be used to filter out traps from the CorreLog server, and discussed in the next section.

Section 3: Software Operation

The CorreLog SNMP Trap Monitor software allows the user to correlate message information, sent by devices in the form of SNMP traps. This provides an extra capability to gather certain classes of information in a consistent way, including "coldstart" and "warmstart" messages, changes to device information, as well as all changes to interface states. The actual capability and range of messages depends upon the information that the SNMP agent vendor has implemented; this can be quite extensive in the case of network devices such as routers and switches.

The CorreLog SNMP Trap Monitor program requires very limited operating notes. Once the program is installed, it makes use of reasonable default values. The operator only needs to direct SNMP traps to the CorreLog IP address, as documented by the vendor. Once these traps are received, they will appear as syslog messages in the CorreLog system, permitting the operator to create Threads and Alerts for the data, and correlate this information with other log messages associated with the device.

This section provides a description of these optional software elements, their usage, and other considerations, including screenshots and explanation of monitor configuration values.

SNMP Trap Parameters Screen

As part of the Windows installation, a new tab is created in the "Message > Config" section of the CorreLog web interface, which permits the user to configure various parameters associated with the SNMP Trap Monitor background program. This screen is available only to CorreLog administrators, and is depicted below:

CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Search Devices Users Facilities Severities Aux Config/
Filters Overrides/ Traps Forwarding Colors Parms
Refresh / Edit: Refresh Edit >
Directly Edit Trap Agent Configuration File...
Match SNMP Trap Community *
Output Message Format Ergonomic
Receive Standard Traps True
Use Standard Facility network
Use Standard Severity notice
Receive Enterprise Traps True
Use Enterprise Facility network
Use Enterprise Severity info
Receive Auth Traps True
Include Source IP Address In Message True
Include Trap Community In Message True
Local intranet

The above screen is a standard CorreLog parameter editor screen. The user can click the "Edit" button to edit parameter values. Once the monitor values have been modified, the user clicks on the "Save" button to save the values. These

values are subsequently read by the background process and apply to future SNMP traps received by the program.

Parameters are described as follows:

- **Match SNMP Trap Community.** This value is a keyword or wildcard that must match the "community" of any received trap. The default value of "*" matches any trap community. The user can limit the reception of traps to a particular trap community. Note that the "community" string is often used as a password when configuring the trap destination for a particular device, and is a standard SNMP configuration item for SNMP agents of all types. The user should consult the documentation of the particular SNMP agent or trap sender for notes on how to configure the source trap community.

- **Output Message Format.** This setting allows control over the message format, and how the SNMP trap is converted to a syslog message. The default setting of "Ergonomic" parses any textual variable bindings from the trap, and appends these values to the syslog message. Other options include "Bind Ordered", "Brief", and "Default". These options are documented in the next section.

- **Receive Standard Traps.** This setting controls whether standard "coldstart", "warmstart", "linkup", "linkdown" and "neighborloss" traps are converted to syslog messages. Most agents generate these standard traps. By default, these traps are converted to syslog messages by the CO-systrap.exe background process, and will appear in CorreLog as a syslog message.

- **Use Standard Facility.** This setting controls the "Facility" associated with standard traps. By default, the "Network" facility is used when an SNMP trap is converted to a syslog message. The operator can select some other value for standard SNMP traps.

- **Use Standard Severity.** This setting controls the "Severity" associated with standard traps. By default, the "Notice" severity is used when a standard SNMP trap is converted to a syslog message. The operator can select some other severity for standard SNMP traps.

- **Receive Enterprise Traps.** This setting controls whether enterprise traps (which are defined by the SNMP agent vendor) are converted to syslog messages. By default, these traps are converted, and will appear in CorreLog as a syslog message. To disable the transmission of enterprise traps, this value can be set to "False", and enterprise traps will not be sent to CorreLog.

- **Use Enterprise Facility.** This setting controls the "Facility" associated with enterprise traps. By default, the "Network" facility is used when an SNMP trap is converted to a syslog message. The operator can select some other value for enterprise SNMP traps.

- **User Enteprise Severity.** This setting controls the "Severity" associated with enterprise traps. By default, the "Info" severity is used when an enterprise SNMP trap is converted to a syslog message. The operator can select some other severity for enterprise SNMP traps. Note that enterprise traps can actually be of any particular severity, hence the "Severity Override" facility of CorreLog is often used to set a precise severity for enterprise traps.

- **Receive Auth Traps.** This setting controls whether "Authentication" traps are converted to syslog messages. These special types of traps indicate that a network manager has attempted to access the agent using an improper community name. This is such a common occurrence (on some networks) that the CorreLog operator can specifically disable the issuance of an "Auth Type" trap. By default, CorreLog reports "Auth Type" traps with the same facility and severity as a standard trap.

Output Message Formats

SNMP trap messages are generally not human readable. CorreLog converts the trap into a syslog message based upon various techniques, including parsing the optional variable bindings associated with many SNMP traps to compose a textual message. On the Messages > Config > Traps screen, the operator can specify one of three different message formats as follows:

- **Ergonomic Format.** This output format consists of the enterprise ID, followed by the trap identifier, followed by any textual bindings. If there are bindings, which are not textual, these bindings are appended to the message. This is the default format, which is often the most human readable type of message, and the message, which is the easiest to correlate.

- **Brief Format.** This output format is the least readable and briefest type of format. The format consists of a series of object ID and values, in the order, which they were listed, omitting any values that are null or non-textual.

- **Bind Ordered Format.** This output format is similar to the "Ergonomic" format (above) except any variable bindings are listed in the order in which they were received (not necessarily the most logical or pertinent order to the user. This value may be useful when normalizing messages, or when

a particular message binding is being parsed or tested by the correlation engine.

- **Include Source IP Address In Message.** This setting will add the trap address to the message. This may be useful if the message address has been overridden by other parts of CorreLog. The source IP address of the message, contained in the trap, is added to the message

- **Include Trap Community In Message.** This setting will add the trap community value to the message, useful for identifying the particular community name. Note that the trap community can be used to filter out traps from the receiver, but by default the system accepts traps from any location. If the value of "Match SNMP Trap Community" contains a wildcard, this setting allows the operator to identify the exact community name contained in the trap.

The "Default" setting in the "Output Message Format" selects the default setting for the system, which is the "Ergonomic Format" on most systems. Generally, the user should start with the "Ergonomic Format", and make adjustments only if specifically required by the site.

Creating Threads, Tickets, and Alerts

The basic method for correlating the SNMP Trap messages is no different that the techniques discussed elsewhere. The basic steps are provided below.

1. The operator creates a thread to tabulate the messages sent by the monitor using the "Correlation > Threads > Add New" screen. This screen is used to collect all the messages of a particular type (such as all messages with "Cisco" in their title, possibly further qualified by a particular address group, severity, or time of day.)

2. The operator creates an Alert for the thread counter using the "Alerts > Counters > Add New" screen. This alert will send a syslog message back to the main list of messages when one or more messages are received during an interval of time. As is always the case, when an alert is triggered, a single message is sent back to CorreLog, and a single ticket is opened while the alert is set. (See additional notes below.)

3. The operator optionally identifies an "Assignee" for the alert via the "Alerts > Counters > Add New" screen. This causes a ticket to be opened on the system, and assigned to a particular user or a ticket group. The user can assign a ticket to any existing user, or ticket group.

4. The operator optionally adds a "Ticket Action" to the system, which sends e-mail (or performs some other action) when a new ticket is opened on the

system, providing a real-time indication that a particular SNMP trap has been received. This message will typically contain the descriptive text entered by the operator when the alert was created, which may be slightly (or totally) different than the originating trap message.

Note that SNMP traps do not have severity and facility information associated with them. The user specifies this information on the "Messages > Config > Parameters" screen, and can further adjust facility and severities using the "Messages > Config > Overrides" facility. This provides a method of targeting, filtering, and correlating SNMP trap messages based upon complex match patterns and other criteria.

Consult the "CorreLog User Reference Manual" for more specific help on how to correlate messages, define alerts, and open tickets.

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Alphabetical Index

A

About / 10
Action / 17
Adapter / 19
Address / 6
Administrative / 9
Alerts / 9 13 17
Alphabetical Index / 19
Assignee / 17
Auth / 16
Authentication / 16

B

Basics / 6
Basics, SNMP Trap / 6
Bind / 15 16
Binding / 7
Bindings / 7
Block / 8

C

Cisco / 17
Co-systrapexe / 6 7 8 10 11 15

Co-sytrapexe / 8
Comment / 10
Community / 6 7 11 15
Components / 7
Components, SNMP Trap Monitor System Software / 7
Config / 5 7 8 9 11 14 16 17
Configuration / 7 11
Configuration, SNMP Trap Monitor / 11
Correlation / 17
Correlog / 5 6 7 8 9 10 11 13 14 15 16 17
Creating / 17

D

Data / 7
Default / 15 17
Destination / 7 11
Diagram / 8
Disk / 10
Distribution / 9

E

Enteprise / 16
Enterprise / 6 7 15
Ergonomic / 15 16 17
Existing / 10

F

Facility / 15
False / 15
Firewall / 10
Format / 15 16 17
Formats / 16
Formats, Output Message / 16
Framework / 9

H

How To Use This Manual / 8

I

Identifier / 6
Index / 19

Index, Alphabetical / 19
Info / 16
Installation / 9 10
Installation, Software / 9
Installation, Windows Procedure / 10
Introduction / 5 5

M

Main / 8
Manager / 10 11
Manual / 8 10 17
Manual, How To Use This / 8
Message / 14 15 16 17
Message, Output Formats / 16
Messages / 5 7 8 9 11 16 17

N

Name / 6
Notice / 15
Number / 7

O

Object / 6
Oids / 7
Operation / 6 13
Ordered / 15 16
Output / 15 16 17
Output Message Formats / 16
Overrides / 17
Overview / 6

P

Page / 19
Parameters / 14 15 17
Procedure / 10
Procedure, Windows Installation / 10
Program / 7

R

Receive / 15 16
Reference / 10 17

Requirements / 10
Restart / 11
Routers / 8

S

SNMP Trap Basics / 6
SNMP Trap Monitor Configuration / 11
SNMP Trap Monitor System Software Components / 7
Save / 14
Schedule / 7 10
Server / 5 8 9 10
Service / 9 10 11
Services / 10 11
Severity / 15 16
Software / 7 9 13
Software, SNMP Trap Monitor System Components / 7
Software Installation / 9
Software Operation / 13
Switches / 8
Syslog / 5 15 16 17
System / 7 8 10
System, SNMP Trap Monitor Software Components / 7

T

Task / 10 11
Threads / 9 13 17
Ticket / 9 17
Tickets / 17
Trap / 5 6 7 8 9 10 11 13 14 15 17 19
Trap, SNMP Basics / 6
Trap, SNMP Monitor Configuration / 11
Trap, SNMP Monitor System Software Components / 7
Traps / 7 8 9 11 15 16

U

User / 8 10 16 17
Users / 7

V

Variable / 7
Verify / 10 11
Virus / 10

W

Windows / 7 8 9 10 11 14
Windows Installation Procedure / 10
Winzip / 7 9